



Panduan Manajemen Desktop

Business Desktops

Nomor Suku Cadang untuk Dokumen ini: 361202-BW1

Mei 2004

Panduan ini berisi definisi dan petunjuk untuk menggunakan fitur keamanan dan fitur Intelligent Manageability yang sudah diinstal pada model-model tertentu.

© Hak cipta 2004 Hewlett-Packard Development Company, L.P.
Informasi yang terdapat dalam dokumen ini dapat berubah sewaktu-waktu tanpa pemberitahuan.

Microsoft dan Windows adalah merek dagang milik Microsoft Corporation di Amerika Serikat dan negara/kawasan lainnya.

Satu-satunya jaminan atas produk dan layanan HP tercantum dalam pernyataan jaminan yang menyertai produk dan layanan tersebut. Tidak ada bagian dari dokumen ini yang dapat dianggap sebagai jaminan tambahan. HP tidak bertanggung jawab atas kesalahan teknis maupun editorial ataupun kekurangan yang tercantum dalam perjanjian ini.

Dokumen ini berisi informasi hak milik yang dilindungi oleh hak cipta. Dokumen ini tidak boleh difotokopi, diperbanyak, atau diterjemahkan ke bahasa lain tanpa persetujuan tertulis di muka dari Hewlett-Packard Company.



PERINGATAN: Teks yang diuraikan dengan cara ini menunjukkan bahwa jika petunjuk tidak dilaksanakan, dapat mengakibatkan cedera tubuh atau hilangnya nyawa.



AWAS: Teks yang diuraikan dengan cara ini menunjukkan bahwa jika petunjuk tidak dilaksanakan, dapat mengakibatkan kerusakan perangkat atau hilangnya informasi.

Panduan Manajemen Desktop

Business Desktops

Edisi Pertama (Mei 2004)

Nomor Suku Cadang untuk Dokumen ini: 361202-BW1

Daftar Isi

Panduan Manajemen Desktop

Konfigurasi dan Penerapan Awal	2
Penginstalan Sistem Jarak Jauh	3
Pemutakhiran (Update) dan Manajemen Perangkat Lunak	4
HP Client Manager Software	4
Altiris Client Management Solutions	4
System Software Manager	6
Proactive Change Notification	6
Subscriber's Choice	7
ROM Flash	7
Remote ROM Flash	8
HPQFlash	8
FailSafe Boot Block ROM	8
Membuat Replika Konfigurasi Penyiapan	10
Tombol Daya Fungsi Ganda	21
Situs World Wide Web	22
Perangkat Pembangun dan Mitra	22
Penelusuran Aset dan Keamanan	23
Pengamanan dengan Sandi	29
Menetapkan Sandi Penyiapan Menggunakan Computer Setup	29
Menetapkan Sandi Power-On Menggunakan Computer Setup	30
DriveLock	35
Smart Cover Sensor	38
Smart Cover Lock	39
Master Boot Record Security	42
Sebelum Memformat atau Memasang Partisi pada Disk yang Dapat Di-boot Saat Ini	44
Pemasangan Kunci Kabel	44
Teknologi Identifikasi Sidik Jari	45

Pemberitahuan dan Pemulihan Kesalahan	45
Sistem Perlindungan Drive	46
Catu Daya yang Dapat Menahan Lonjakan Arus	46
Sensor Panas	46

Indeks

Panduan Manajemen Desktop

HP Intelligent Manageability memberikan solusi berbasis-standar untuk mengelola dan mengontrol PC desktop, workstation, dan notebook dalam lingkungan jaringan. HP memelopori pengelolaan desktop pada tahun 1995 dengan mengeluarkan komputer pribadi desktop yang sepenuhnya dapat dikelola. HP adalah pemegang paten teknologi manageability (kemampuan untuk dikelola). Sejak itu, HP memimpin upaya dalam industri untuk mengembangkan standar dan prasarana yang diperlukan untuk secara efektif menerapkan, mengkonfigurasi, dan mengelola PC desktop, workstation, dan notebook. HP secara erat bekerja bersama penyedia solusi perangkat lunak manajemen terkemuka dalam industri ini untuk memastikan kompatibilitas antara Intelligent Manageability dan produk-produk ini. Intelligent Manageability adalah aspek penting dari komitmen luas kami untuk memberikan PC Lifecycle Solutions yang membantu Anda dalam keempat tahap siklus hidup PC desktop — perencanaan (planning), penerapan (deployment), manajemen (management), dan transisi (transitions).

Kapabilitas dan fitur utama dari manajemen desktop adalah:

- Konfigurasi dan penerapan awal
- Penginstalan sistem jarak jauh
- Pemutakhiran (update) dan manajemen perangkat lunak
- ROM flash
- Penelusuran dan pengamanan aset
- Pemberitahuan dan pemulihan kegagalan



Dukungan bagi fitur-fitur khusus yang diuraikan dalam panduan ini dapat bervariasi berdasarkan model atau versi perangkat lunak.

Konfigurasi dan Penerapan Awal

Komputer dilengkapi dengan image perangkat lunak sistem yang sudah diinstal sebelumnya. Setelah melalui proses “pembukaan kemasan” perangkat lunak, komputer siap digunakan.

Anda dapat memilih untuk mengganti image perangkat lunak pra-instal (preinstalled) dengan sekumpulan perangkat lunak sistem dan aplikasi yang sudah dikustomisasi (disesuaikan). Ada beberapa metode untuk menerapkan image perangkat lunak hasil kustomisasi. Yaitu:

- Menginstal aplikasi perangkat lunak tambahan setelah membuka kemasan image perangkat lunak pra-instal tersebut.
- Menggunakan alat bantu penerapan perangkat lunak, seperti Altiris Deployment Solution™, untuk mengganti perangkat lunak pra-instal dengan image perangkat lunak kustomisasi.
- Menggunakan proses cloning (penggandaan) disk untuk menyalin isi suatu hard drive ke hard drive lainnya.

Metode penerapan terbaik tergantung pada lingkungan dan proses teknologi informasi Anda. Bagian PC Deployment pada situs Web HP Lifecycle Solutions (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>) berisi informasi yang dapat membantu Anda memilih metode penerapan yang terbaik.

CD *Restore Plus!*, penyiapan berbasis-ROM, serta perangkat keras ACPI menyediakan bantuan lebih lanjut dalam hal pemulihan perangkat lunak sistem, manajemen konfigurasi dan pemecahan masalah, serta manajemen daya.

Penginstalan Sistem Jarak Jauh

Dengan Penginstalan Sistem Jarak Jauh (Remote System Installation), Anda dapat menghidupkan dan menyiapkan sistem menggunakan informasi perangkat lunak dan konfigurasi yang terletak pada server jaringan dengan menjalankan Preboot Execution Environment (PXE). Fitur Remote System Installation biasanya digunakan sebagai alat bantu penyiapan dan konfigurasi sistem, dan dapat digunakan untuk tindakan-tindakan berikut:

- Memformat hard drive
- Menerapkan image perangkat lunak pada satu PC baru atau lebih
- Secara jarak jauh melakukan pemutakhiran BIOS sistem dalam flash ROM (“[Remote ROM Flash](#)” pada [halaman 8](#))
- Mengkonfigurasi setelan BIOS sistem

Untuk memulai Remote System Installation, tekan **F12** bila muncul pesan F12 = Network Service Boot pada sudut kanan bawah layar logo HP. Ikuti petunjuk pada layar untuk melanjutkan proses tersebut. Urutan boot (boot order) default adalah setelan konfigurasi BIOS yang dapat diubah agar selalu mencoba boot PXE.

HP dan Altiris telah bermitra untuk menyediakan alat bantu yang dirancang untuk memudahkan dan mempercepat pekerjaan menerapkan dan mengelola PC korporasi, sehingga pada akhirnya menurunkan biaya total kepemilikan dan menjadikan PC HP sebagai PC klien yang paling mudah dikelola dalam lingkungan perusahaan.

Pemutakhiran (Update) dan Manajemen Perangkat Lunak

HP menyediakan beberapa alat bantu untuk mengelola dan memutakhirkan perangkat lunak pada desktop dan workstation — HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification; dan Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) membantu pelanggan HP dalam mengelola aspek perangkat keras dari komputer klien mereka dengan fitur-fitur yang mencakup:

- Menampilkan secara rinci inventori perangkat keras untuk keperluan manajemen aset
- Pemantauan dan diagnostika pemeriksaan kesehatan PC
- Pemberitahuan proaktif mengenai perubahan perangkat keras
- Sistem pelaporan yang dapat diakses di Web, mengenai informasi bisnis yang kritis seperti mesin-mesin yang dilengkapi peringatan panas, peringatan memori, dan banyak lagi
- Memutakhirkan secara jarak jauh perangkat lunak sistem seperti driver perangkat dan ROM BIOS
- Penggantian urutan boot secara jarak jauh

Untuk informasi mengenai HP Client Manager, kunjungi http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

HP dan Altiris telah bermitra untuk menyediakan solusi manajemen sistem komprehensif yang sangat terpadu untuk mengurangi biaya pembelian PC klien HP. HP Client Manager Software adalah landasan untuk Altiris Client Management Solutions tambahan yang menangani:

- Manajemen Inventori dan Aset
 - ❑ Kepatuhan terhadap lisensi perangkat lunak

- ☐ Penelusuran dan pelaporan PC
- ☐ Kontrak sewa-guna, menetapkan penelusuran aset
- Penerapan dan Migrasi
 - ☐ Migrasi Microsoft Windows XP Professional atau Home Edition
 - ☐ Penerapan sistem
 - ☐ Migrasi personalitas
- Help Desk dan Resolusi Masalah
 - ☐ Mengelola tiket help desk
 - ☐ Mengatasi masalah jarak jauh
 - ☐ Penyelesaian masalah jarak jauh
 - ☐ Pemulihan bencana klien
- Manajemen Perangkat Lunak dan Operasi
 - ☐ Manajemen desktop berkelanjutan
 - ☐ Penerapan perangkat lunak sistem HP
 - ☐ Penyembuhan sendiri (self-healing) oleh aplikasi

Untuk informasi lebih lanjut dan rincian mengenai cara men-download solusi Altiris versi evaluasi 30-hari yang fungsinya lengkap, kunjungi

<http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

Pada sebagian model desktop dan notebook, disertakan agen manajemen Altiris sebagai bagian dari image yang dimuatkan pabrik. Dengan agen ini, komputer dapat berkomunikasi dengan Altiris Development Solution yang dapat digunakan untuk menyelesaikan penerapan perangkat keras baru atau migrasi personalitas ke sistem operasi baru menggunakan wisaya (wizard) yang mudah diikuti. Solusi Altiris menyediakan fitur distribusi perangkat lunak yang mudah digunakan. Bila digunakan bersama System Software Manager, atau HP Client Manager Software, administrator juga dapat memutakhirkan ROM BIOS dan perangkat lunak driver perangkat dari sebuah konsol sentral.

Untuk informasi lebih jauh, kunjungi

<http://h18000.www1.hp.com/im/index.html>.

System Software Manager

System Software Manager (SSM) adalah utilitas yang memungkinkan Anda untuk memutakhirkan perangkat lunak di level sistem sekaligus pada beberapa sistem. Bila dijalankan pada sistem klien PC, SSM mendeteksi versi perangkat keras dan perangkat lunak, kemudian memutakhirkan perangkat lunak yang sesuai dari suatu tempat penyimpanan sentral, yang juga dikenal sebagai penyimpanan file. Versi driver yang didukung oleh SSM ditandai dengan ikon khusus pada situs Web tempat men-download driver, serta pada CD perangkat lunak pendukung. Untuk men-download utilitas ini atau untuk mendapatkan informasi lebih lanjut mengenai SSM, kunjungi <http://www.hp.com/go/ssm>.

Proactive Change Notification

Program Proactive Change Notification (pemberitahuan perubahan proaktif) menggunakan situs Web Subscriber's Choice untuk secara proaktif dan otomatis:

- Mengirimkan email Proactive Change Notification (PCN) yang berisi pemberitahuan mengenai perubahan perangkat keras dan perangkat lunak pada sebagian besar komputer dan server komersial, hingga 60 hari di muka.
- Mengirimkan kepada Anda email yang berisi Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins, dan pemberitahuan Driver untuk sebagian besar komputer dan server komersial.

Andalah yang akan membuat profil Anda sendiri untuk memastikan bahwa Anda hanya menerima informasi yang relevan dengan lingkungan IT tertentu saja. Untuk mengetahui lebih jauh mengenai program Proactive Change Notification dan untuk membuat profil sesuai kehendak, kunjungi <http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

Subscriber's Choice

Subscriber's Choice adalah layanan berbasis-klien dari HP. Berdasarkan profil Anda, HP akan mengirimkan tip-tip produk, artikel, dan/atau pemberitahuan driver dan dukungan yang disesuaikan kebutuhan Anda. Pemberitahuan/peringatan driver dan dukungan (Driver and Support Alerts/Notifications) Subscriber's Choice akan mengirimkan email berisi pemberitahuan bahwa informasi yang Anda pilih pada profil sudah tersedia untuk dilihat dan diambil. Untuk mengetahui lebih lanjut mengenai Subscriber's Choice dan untuk membuat profil sesuai kehendak, kunjungi <http://h30046.www3.hp.com/subhub.php>.

ROM Flash

Komputer ini dilengkapi dengan flash ROM (read only memory) yang dapat diprogram. Dengan menetapkan sandi penyiapan (setup) pada Computer Setup (F10) Utility, Anda dapat melindungi ROM agar tidak dimutakhirkan atau ditimpa secara tidak sengaja. Hal ini penting untuk memastikan integritas operasi komputer tersebut. Jika Anda perlu atau ingin meningkatkan ROM, Anda dapat:

- Memesan disket ROMPaq yang sudah ditingkatkan dari HP.
- Men-download image ROMPaq terbaru dari halaman driver dan dukungan HP, <http://www.hp.com/support/files>.



AWAS: Untuk perlindungan ROM yang maksimum, pastikan untuk menetapkan sandi penyiapan. Sandi penyiapan akan mencegah peningkatan ROM yang tidak berwenang. System Software Manager memungkinkan administrator sistem untuk mengeset sandi penyiapan sekaligus pada satu PC atau lebih. Untuk informasi lebih jauh, kunjungi <http://www.hp.com/go/ssm>.

Remote ROM Flash

Remote ROM Flash memungkinkan administrator sistem untuk secara aman meningkatkan ROM pada komputer HP jarak jauh, langsung dari konsol manajemen jaringan sentral. Dengan membiarkan administrator sistem untuk menjalankan tindakan ini secara jarak jauh, pada banyak komputer dan komputer pribadi (PC), akan menghasilkan penerapan yang konsisten dan kontrol yang lebih baik terhadap image PC ROM HP pada jaringan tersebut. Juga meningkatkan produktivitas dan menurunkan biaya pemilikan.



Untuk dapat menggunakan Remote ROM Flash, komputer harus didayai atau dihidupkan melalui Remote Wakeup.

Untuk informasi lebih lanjut mengenai Remote ROM Flash, lihat HP Client Manager Software atau System Software Manager pada <http://h18000.www1.hp.com/im/prodinfo.html>.

HPQFlash

Utilitas HPQFlash digunakan untuk secara lokal memutakhirkan atau mengembalikan ROM sistem pada PC individual melalui sistem operasi Windows.

Untuk informasi lebih jauh mengenai HPQFlash, kunjungi <http://www.hp.com/support/files>, kemudian masukkan nama komputer bila diminta.

FailSafe Boot Block ROM

FailSafe Boot Block ROM memungkinkan pemulihan sistem jika sampai terjadi kegagalan ROM flash, di mana hal ini sangat kecil kemungkinannya, misalnya jika daya listrik mati pada saat ROM sedang ditingkatkan. Boot Block adalah bagian ROM yang diproteksi flash, yang memeriksa flash ROM sistem yang valid bila daya listrik dialirkan ke sistem tersebut.

- Jika ROM sistem valid, sistem akan dimulai secara normal.
- Jika ROM sistem gagal pada pengecekan validasi, FailSafe Boot Block ROM memberikan dukungan yang cukup untuk memulai sistem dari disket ROMPaq, yang akan memrogram ROM sistem dengan image yang valid.



Beberapa model juga mendukung pemulihan dari CD ROMPaq. Pada sejumlah model tertentu, image ISO ROMPaq disertakan dalam ROM softpaqs yang dapat di-download.

Bila boot block tersebut mendeteksi adanya ROM sistem yang tidak valid, lampu LED daya sistem akan berkedip MERAH 8 kali, satu kali per detik, diikuti dengan jeda 2 detik. Juga akan terdengar 8 bunyi bip sekaligus. Sebuah pesan mode pemulihan Boot Block akan ditampilkan di layar (pada sebagian model saja).

Untuk memulihkan sistem setelah memasuki mode pemulihan Boot Block, lakukan langkah-langkah berikut:

1. Jika ada disket di dalam drive disket atau CD dalam drive CD, keluarkan disket dan CD, kemudian matikan daya.
2. Masukkan disket ROMPaq ke drive disket tersebut atau, jika diizinkan pada komputer tersebut, masukkan CD ROMPaq ke dalam drive CD.
3. Hidupkan komputer.

Jika tidak ada disket ROMPaq atau CD ROMPaq, Anda akan diminta untuk memasukkan disket atau CD tersebut dan menghidupkan ulang komputer.

Jika sandi penyiapan sudah ditetapkan, lampu Caps Lock akan menyala dan Anda diminta untuk memasukkan sandi.

4. Masukkan sandi penyiapan.

Jika sistem berhasil dimulai dari disket dan berhasil memrogram ulang ROM, maka ketiga lampu papan ketik akan menyala. Keberhasilan ini juga akan ditandai oleh serangkaian bunyi bip yang nadanya makin tinggi.

5. Lepaskan disket atau CD, kemudian matikan daya.
6. Hidupkan lagi daya, untuk menghidupkan ulang komputer.

Tabel berikut berisi daftar berbagai kombinasi lampu papan ketik yang digunakan oleh Boot Block ROM (bila ada papan ketik PS/2 yang terhubung ke komputer), dan berisi uraian arti dan tindakan untuk setiap kombinasi tersebut.

Kombinasi Lampu Papan Ketik yang Digunakan oleh Boot Block ROM

Mode FailSafe Boot Block	Warna Lampu LED Papan Ketik	Aktivitas LED Papan Ketik	Keadaan/Pesan
Num Lock	Hijau	Menyala	Disket ROMPaq atau CD ROMPaq tidak ada, rusak, atau drive tidak siap.
Caps Lock	Hijau	Menyala	Masukkan sandi.
Num, Caps, Scroll Lock	Hijau	Berkedip secara berurutan, satu per satu—N, C, SL	Papan ketik terkunci dalam mode jaringan.
Num, Caps, Scroll Lock	Hijau	Menyala	Boot Block ROM Flash berhasil. Matikan daya, kemudian hidupkan lagi untuk melakukan boot ulang.

 Pada papan ketik USB, lampu diagnostik tidak berkedip.

Membuat Replika Konfigurasi Penyiapan

Dengan prosedur berikut, seorang administrator dapat dengan mudah menyalin suatu konfigurasi penyiapan ke komputer lain yang modelnya sama. Dengan demikian, konfigurasi multi komputer dapat dilakukan secara lebih cepat dan lebih konsisten.



Kedua prosedur ini memerlukan drive disket atau perangkat media flash USB yang didukung, seperti HP Drive Key.

Menyalin ke Satu Komputer



AWAS: Konfigurasi penyiapan adalah khusus untuk setiap model. Kesalahan (corruption) sistem file dapat terjadi jika komputer sumber dan tujuan tidak sama modelnya. Misalnya, jangan menyalin konfigurasi penyiapan dari dc7100 Ultra-Slim Desktop ke dx6100 Slim Tower.

1. Pilih konfigurasi penyiapan yang akan disalin. Matikan komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Shut Down**.
2. Jika Anda menggunakan perangkat media flash USB, masukkanlah media tersebut sekarang.
3. Hidupkan komputer.
4. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

5. Jika Anda menggunakan disket, masukkan disket sekarang.
6. Klik **File > Replicated Setup > Save to Removable Media**. Ikuti petunjuk di layar untuk membuat disket atau perangkat media flash USB konfigurasi.
7. Matikan komputer yang akan dikonfigurasi, kemudian masukkan disket konfigurasi atau perangkat media flash USB tersebut.
8. Hidupkan komputer yang akan dikonfigurasi.
9. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.
10. Klik **File > Replicated Setup > Restore from Removable Media**, kemudian ikuti petunjuk di layar.
11. Hidupkan ulang komputer bila konfigurasi selesai.

Menyalin ke Lebih dari Satu Komputer



AWAS: Konfigurasi penyiapan adalah khusus untuk setiap model. Kesalahan (corruption) sistem file dapat terjadi jika komputer sumber dan tujuan tidak sama modelnya. Misalnya, jangan menyalin konfigurasi penyiapan dari dc7100 Ultra-Slim Desktop ke dx6100 Slim Tower.

Metode ini akan memakan waktu sedikit lebih lama untuk menyiapkan disket konfigurasi atau perangkat media flash USB tersebut, tapi penyalinan konfigurasi ke komputer tujuan menjadi lebih cepat.



Dalam prosedur ini, diperlukan sebuah disket yang dapat di-boot untuk membuat perangkat media flash USB yang dapat di-boot. Jika Windows XP tidak tersedia untuk dapat membuat disket yang dapat di-boot, gunakan metode untuk menyalin ke satu komputer (lihat [“Menyalin ke Satu Komputer” pada halaman 11](#)).

1. Buatlah disket atau perangkat media flash USB yang dapat di-boot. Lihat [“Perangkat Media Flash USB yang Didukung” pada halaman 14](#) atau [“Perangkat Media Flash USB yang Tidak Didukung” pada halaman 17](#).
-



AWAS: Tidak semua komputer dapat di-boot dari perangkat media flash USB. Jika urutan boot default pada Computer Setup (F10) Utility mencantumkan perangkat USB pada urutan sebelum hard drive, maka komputer dapat di-boot dari perangkat media flash USB. Jika tidak, harus digunakan disket yang dapat di-boot.

2. Pilih konfigurasi penyiapan yang akan disalin. Matikan komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Shut Down**.
3. Jika Anda menggunakan perangkat media flash USB, masukkanlah media tersebut sekarang.
4. Hidupkan komputer.

5. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

6. Jika Anda menggunakan disket, masukkan disket sekarang.
7. Klik **File > Replicated Setup > Save to Removable Media**. Ikuti petunjuk di layar untuk membuat disket atau perangkat media flash USB konfigurasi.
8. Download utilitas BIOS untuk membuat replika penyiapan (repset.exe), kemudian salinlah ke disket atau perangkat media flash USB tersebut. Untuk mendapatkan utilitas ini, kunjungi <http://welcome.hp.com/support/files>, kemudian masukkan nomor model komputer.
9. Pada disket konfigurasi atau perangkat media flash USB konfigurasi tersebut, buat file autoexec.bat yang berisi perintah berikut:
repset.exe
10. Matikan komputer yang akan dikonfigurasi. Masukkan disket konfigurasi atau perangkat media flash USB konfigurasi tersebut, kemudian hidupkan komputer. Utilitas konfigurasi akan dijalankan secara otomatis.
11. Hidupkan ulang komputer bila konfigurasi selesai.

Membuat Perangkat yang Dapat Di-boot

Perangkat Media Flash USB yang Didukung

Perangkat yang didukung, seperti HP Drive Key atau Disjoined, memiliki image yang sudah diinstal untuk memudahkan proses untuk menjadikannya dapat di-boot. Jika perangkat media flash USB yang digunakan tersebut tidak memiliki image ini, gunakan prosedur lain pada bagian ini (lihat [“Perangkat Media Flash USB yang Tidak Didukung”](#) pada halaman 17).



AWAS: Tidak semua komputer dapat di-boot dari perangkat media flash USB. Jika urutan boot default pada Computer Setup (F10) Utility mencantumkan perangkat USB pada urutan sebelum hard drive, maka komputer dapat di-boot dari perangkat media flash USB. Jika tidak, harus digunakan disket yang dapat di-boot.

Untuk membuat perangkat media flash USB, Anda harus memiliki:

■ Salah satu dari sistem-sistem berikut:

- ☐ HP Compaq Business Desktop dc7100 series
- ☐ HP Compaq Business Desktop dx6100 series
- ☐ HP Compaq Business Desktop d530 Series - Ultra-Slim Desktop, Small Form Factor, atau Convertible Minitower
- ☐ Compaq Evo D510 Ultra-slim Desktop
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor

Bergantung pada BIOS individual, sistem di masa depan mungkin mendukung proses boot ke perangkat media flash USB.



AWAS: Jika Anda menggunakan komputer selain dari yang disebutkan di atas, pastikan bahwa dalam urutan boot default pada Computer Setup (F10) Utility, perangkat USB tersebut tercantum sebelum hard drive.

- Salah satu dari modul-modul penyimpanan berikut:
 - ☐ 16MB HP Drive Key
 - ☐ 32MB HP Drive Key
 - ☐ 32MB DiskOnKey
 - ☐ 64MB HP Drive Key
 - ☐ 64MB DiskOnKey
 - ☐ 128MB HP Drive Key
 - ☐ 128MB DiskOnKey
 - ☐ 256MB HP Drive Key
 - ☐ 256MB DiskOnKey
- Disket DOS yang dapat di-boot dan dilengkapi program FDISK dan SYS. Jika SYS tidak tersedia, FORMAT dapat digunakan, namun semua file yang ada pada perangkat media flash USB akan hilang.
 1. Matikan komputer.
 2. Masukkan perangkat media flash USB ke salah satu porta USB pada komputer, kemudian lepaskan semua perangkat penyimpanan USB lainnya kecuali drive disket USB.
 3. Masukkan disket DOS yang dapat di-boot yang disertai FDISK.COM dan salah satu dari SYS.COM atau FORMAT.COM ke dalam drive disket, kemudian hidupkan komputer untuk mem-boot disket DOS tersebut.
 4. Jalankan FDISK dari prompt A:\ dengan mengetikkan **FDISK** dan menekan Enter. Jika diminta, klik **Yes (Y)** untuk memfungsikan dukungan untuk disk besar.
 5. Masukkan Choice [**5**] untuk menampilkan drive yang terdapat pada sistem tersebut. Perangkat media flash USB adalah drive yang ukurannya mendekati ukuran salah satu drive yang tercantum. Biasanya merupakan drive yang terakhir dalam daftar. Catatlah huruf pengenalan drive tersebut.

Drive perangkat media flash USB: _____



AWAS: Jika tidak ada yang cocok dengan perangkat media flash USB, jangan melanjutkan. Dapat terjadi kehilangan data. Periksa semua porta USB, apakah ada perangkat penyimpanan tambahan. Jika ada, lepaskan, lakukan boot ulang komputer, kemudian lanjutkan dari langkah 4. Jika tidak ada, berarti sistem tidak mendukung perangkat media flash USB tersebut, atau perangkat media flash USB tersebut rusak. JANGAN melanjutkan untuk mengupayakan agar perangkat media flash USB tersebut bisa di-boot.

6. Keluarlah dari FDISK dengan menekan tombol **Esc** untuk kembali ke prompt A:\.
 7. Jika disket DOS yang dapat di-boot tersebut berisi SYS.COM, lanjutkan ke langkah 8. Jika tidak, lanjutkan ke langkah 9.
 8. Pada prompt A:\, masukkan **SYS x:** di mana x adalah huruf pengenalan drive yang dicatat di atas.
-



AWAS: Pastikan Anda memasukkan huruf pengenalan drive yang benar untuk perangkat media flash USB tersebut.

Setelah file sistem ditransfer, SYS akan kembali ke prompt A:\. Lanjutkan ke langkah 13.

9. Salinlah file yang akan dipertahankan dari perangkat media flash USB ke direktori sementara pada drive lainnya (misalnya, hard drive internal sistem tersebut).
 10. Pada prompt A:\, masukkan **FORMAT /S X:** di mana x adalah huruf pengenalan drive yang dicatat di atas.
-



AWAS: Pastikan Anda memasukkan huruf pengenalan drive yang benar untuk perangkat media flash USB tersebut.

FORMAT akan menampilkan sebuah peringatan atau lebih, dan akan selalu bertanya apakah Anda ingin melanjutkan. Masukkan **Y** setiap kali ditanya. FORMAT akan memformat perangkat media flash USB tersebut, menambahkan file sistem, dan meminta Volume Label.

11. Tekan **Enter** jika Anda tidak mau memberi label, atau masukkan nama label jika dikehendaki.

12. Salin file yang disimpan pada langkah 9 tadi, kembali ke perangkat media flash USB.
13. Keluarkan disket, lalu boot ulang komputer. Komputer akan mem-boot ke perangkat media flash USB sebagai drive C.



Urutan boot default bervariasi dari komputer ke komputer, dan urutan ini dapat diubah dalam Computer Setup (F10) Utility.

Jika Anda pernah menggunakan versi DOS dari Windows 9x, mungkin muncul layar logo Windows sesaat. Jika Anda tidak menghendaki layar ini, tambahkan file kosong (zero-length) bernama LOGO.SYS pada direktori akar (root) pada perangkat media flash USB.

Kembali ke [“Menyalin ke Lebih dari Satu Komputer”](#) pada [halaman 12](#).

Perangkat Media Flash USB yang Tidak Didukung



AWAS: Tidak semua komputer dapat di-boot dari perangkat media flash USB. Jika urutan boot default pada Computer Setup (F10) Utility mencantumkan perangkat USB pada urutan sebelum hard drive, maka komputer dapat di-boot dari perangkat media flash USB. Jika tidak, harus digunakan disket yang dapat di-boot.

Untuk membuat perangkat media flash USB, Anda harus memiliki:

■ Salah satu dari sistem-sistem berikut:

- ☐ HP Compaq Business Desktop dc7100 series
- ☐ HP Compaq Business Desktop dx6100 series
- ☐ HP Compaq Business Desktop d530 Series - Ultra-Slim Desktop, Small Form Factor, atau Convertible Minitower
- ☐ Compaq Evo D510 Ultra-slim Desktop
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor

Bergantung pada BIOS individual, sistem di masa depan mungkin mendukung proses boot ke perangkat media flash USB.



AWAS: Jika Anda menggunakan komputer selain dari yang disebutkan di atas, pastikan bahwa dalam urutan boot default pada Computer Setup (F10) Utility, perangkat USB tersebut tercantum sebelum hard drive.

- Disket DOS yang dapat di-boot dan dilengkapi program FDISK dan SYS. Jika SYS tidak tersedia, FORMAT dapat digunakan, namun semua file yang ada pada perangkat media flash USB akan hilang.
- 1. Jika pada sistem yang memiliki drive SCSI, ATA RAID atau SATA terdapat kartu PCI, matikan komputer, kemudian cabutlah kabel daya dari stopkontak.



AWAS: Kabel daya HARUS dilepaskan dari stopkontak.

2. Buka komputer, kemudian lepaskan kartu PCI.
3. Masukkan perangkat media flash USB ke salah satu porta USB pada komputer, kemudian lepaskan semua perangkat penyimpanan USB lainnya kecuali drive disket USB. Tutup penutup komputer.
4. Sambungkan komputer ke sumber listrik, kemudian hidupkan komputer.
5. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

6. Masuklah ke **Advanced > PCI Devices** untuk melumpuhkan kontroler PATA dan SATA. Bila melumpuhkan kontroler SATA, catatlah IRQ yang ditetapkan untuk kontroler tersebut. Anda akan perlu melakukan penetapan ulang IRQ di lain waktu. Keluar dari setup, sambil mengkonfirmasi perubahan.

SATA IRQ: _____

7. Masukkan disket DOS yang dapat di-boot yang disertai FDISK.COM dan salah satu dari SYS.COM atau FORMAT.COM ke dalam drive disket, kemudian hidupkan komputer untuk mem-boot disket DOS tersebut.
8. Jalankan FDISK dan hapus semua partisi pada perangkat media flash USB. Buat partisi baru, kemudian beri tanda sebagai partisi aktif. Keluar dari FDISK dengan menekan tombol **Esc**.
9. Jika sistem tidak secara otomatis dihidupkan ulang ketika keluar dari FDISK, tekan **Ctrl+Alt+Del** untuk mem-boot ulang disket DOS.
10. Pada prompt A:\, masukkan **FORMATC: /S**, kemudian tekan **Enter**. Fitur format akan memformat perangkat media flash USB tersebut, menambahkan file sistem, dan meminta Volume Label.
11. Tekan **Enter** jika Anda tidak mau memberi label, atau masukkan nama label jika dikehendaki.
12. Matikan komputer, lalu cabut kabel daya dari stopkontak. Buka komputer, kemudian pasang lagi kartu PCI yang tadi dilepaskan. Tutup penutup komputer.
13. Sambungkan komputer ke sumber listrik, keluarkan disket, kemudian hidupkan komputer.
14. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.

15. Masuklah ke **Advanced > PCI Devices**, kemudian fungsikan ulang kontroler PATA dan SATA yang dilumpuhkan pada langkah 6. Kembalikan kontroler SATA pada IRQ-nya yang asli.
16. Simpan perubahan, kemudian keluarlah. Komputer akan mem-boot ke perangkat media flash USB sebagai drive C.



Urutan boot default bervariasi dari komputer ke komputer, dan urutan ini dapat diubah dalam Computer Setup (F10) Utility. Lihat *Panduan Penyiapan Komputer* pada *CD Dokumentasi* untuk petunjuk.

Jika Anda pernah menggunakan versi DOS dari Windows 9x, mungkin muncul layar logo Windows sesaat. Jika Anda tidak menghendaki layar ini, tambahkan file kosong (zero-length) bernama LOGO.SYS pada direktori akar (root) pada perangkat media flash USB.

Kembali ke [“Menyalin ke Lebih dari Satu Komputer”](#) pada [halaman 12](#).

Tombol Daya Fungsi Ganda

Bila Advanced Configuration and Power Interface (ACPI) difungsikan, tombol daya dapat berfungsi sebagai saklar hidup/mati atau sebagai tombol siaga (standby). Fitur siaga tidak akan mematikan daya sepenuhnya, namun menyebabkan komputer memasuki keadaan siaga dengan konsumsi daya listrik rendah. Dengan demikian, Anda dapat dengan cepat menurunkan pemakaian daya tanpa harus menutup aplikasi. Anda juga dapat dengan cepat kembali ke keadaan operasional tersebut tanpa kehilangan data apapun.

Untuk mengganti konfigurasi tombol daya, lakukan langkah-langkah berikut:

1. Klik kiri tombol **Start**, kemudian pilih **Control Panel > Power Options**.
2. Pada **Power Options Properties**, pilih tab **Advanced**.
3. Pada bagian **Power Button**, pilih **Stand by**.

Setelah mengkonfigurasi tombol daya agar berfungsi sebagai tombol siaga, tekan tombol daya untuk memasukkan sistem ke keadaan dengan konsumsi daya sangat rendah (siaga). Untuk dengan cepat mengeluarkan sistem dari keadaan siaga dan mengembalikannya ke status daya penuh, tekan lagi tombol tersebut. Untuk sepenuhnya mematikan semua daya ke sistem, tekan terus tombol daya selama empat detik.



AWAS: Jangan menggunakan tombol daya untuk mematikan komputer, kecuali jika komputer tidak bereaksi; mematikan daya tanpa interaksi sistem operasi dapat menyebabkan kerusakan atau hilangnya data pada hard drive.

Situs World Wide Web

Para engineer HP dengan seksama menguji dan melakukan debug perangkat lunak yang dikembangkan HP dan pemasok pihak ketiga, dan mengembangkan perangkat lunak pendukung sistem operasi, untuk memastikan kinerja, kompatibilitas, dan keandalan komputer HP.

Bila melakukan transisi ke sistem operasi yang baru atau yang baru direvisi, penting untuk menerapkan perangkat lunak pendukung yang dirancang untuk sistem operasi tersebut. Jika Anda berencana menjalankan versi Microsoft Windows yang berbeda dari versi yang disertakan dengan komputer tersebut, Anda harus menginstal driver perangkat dan utilitas yang terkait untuk memastikan bahwa semua fitur didukung dan berfungsi dengan benar.

HP telah mengupayakan untuk mempermudah Anda untuk mencari, mengakses, mengevaluasi, dan menginstal perangkat lunak pendukung. Anda dapat men-download perangkat lunak ini dari <http://www.hp.com/support>.

Situs Web ini berisi driver perangkat terbaru, utilitas, dan image ROM terbaru yang dapat di-flash yang diperlukan untuk menjalankan sistem operasi Microsoft Windows mutakhir pada komputer HP.

Perangkat Pembangun dan Mitra

Solusi manajemen HP berintegrasi dengan aplikasi manajemen sistem lainnya, dan didasarkan pada standar industri, seperti:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LAN Technology
- ACPI
- SMBIOS
- Pendukung Pre-boot Execution (PXE)

Penelusuran Aset dan Keamanan

Fitur penelusuran aset (asset tracking) yang disertakan ke dalam komputer ini menyediakan data penelusuran aset utama yang dapat dikelola dengan menggunakan HP Systems Insight Manager, HP Client Manager atau aplikasi manajemen sistem lainnya. Dengan perpaduan yang mulus dan otomatis antara fitur-fitur penelusuran aset dan produk-produk ini, Anda dapat memilih alat bantu manajemen yang paling sesuai dengan lingkungan Anda dan untuk memanfaatkan investasi Anda dalam alat bantu yang sudah ada.

HP juga menawarkan beberapa solusi untuk mengontrol akses ke komponen dan informasi berharga. ProtectTools Embedded Security, jika diinstal, akan mencegah akses tak berwenang menuju data dan akan memeriksa integritas sistem serta memeriksa keabsahan pengguna pihak ketiga yang mencoba mengakses sistem. (Lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi* untuk informasi lebih lanjut.) Fitur-fitur keamanan seperti ProtectTools, Smart Cover Sensor dan Smart Cover Lock, yang tersedia pada model-model tertentu, membantu mencegah akses tak berwenang ke komponen-komponen internal dari komputer pribadi tersebut. Dengan melumpuhkan porta paralel, seri, atau USB, atau dengan melumpuhkan kapabilitas boot media lepasan, Anda dapat melindungi aset data yang berharga. Peringatan Memory Change and Smart Cover Sensor dapat secara otomatis diteruskan ke aplikasi manajemen sistem sehingga perubahan komponen internal komputer dapat diberitahukan secara proaktif.



ProtectTools, Smart Cover Sensor, dan Smart Cover Lock tersedia sebagai perangkat tambahan pada sistem-sistem tertentu.



Gunakan utilitas berikut untuk mengelola setelan sekuriti pada komputer HP:

- Secara lokal, menggunakan Computer Setup Utilities. Lihat *Panduan Utilitas Penyiapan Komputer (F10)* pada *CD Dokumentasi* yang disertakan bersama komputer untuk memperoleh informasi dan petunjuk tambahan mengenai cara penggunaan Computer Setup Utilities.



- Secara jarak jauh, menggunakan HP Client Manager Software atau System Software Manager. Dengan perangkat lunak ini, Anda dapat melakukan penerapan yang aman dan konsisten serta pengontrolan setelan sekuriti dari sebuah utilitas baris-perintah yang sederhana.

Tabel dan bagian berikut ini mengacu ke pengelolaan fitur sekuriti komputer secara lokal melalui Computer Setup (F10) Utilities.



Tinjauan Sekilas mengenai Fitur Sekuriti

Opsi	Uraian
Setup Password	<p>Untuk mengeset dan memfungsikan sandi setup (administrator).</p> <p> Jika sandi setup (penyiapan) ditetapkan, sandi ini diperlukan untuk melakukan perubahan pada opsi-opsi Computer Setup, melakukan flash ROM, dan mengganti setelan plug and play tertentu pada Windows.</p> <p>Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p>
Power-On Password	<p>Untuk menyetel dan memfungsikan sandi power-on.</p> <p>Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p>
Password Options (Pemilihan ini hanya akan muncul jika sandi power-on sudah diset.)	<p>Memungkinkan Anda untuk menentukan apakah sandi diperlukan untuk warm boot (CTRL+ALT+DEL).</p> <p>Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p>
Pre-Boot Authorization	<p>Untuk memfungsikan/melumpuhkan Smart Card untuk digunakan sebagai ganti Power-On Password.</p>
<p> Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada <i>CD Dokumentasi</i>.</p> <p>Dukungan untuk fitur sekuriti dapat bervariasi, bergantung pada konfigurasi komputer tersebut.</p>	



Tinjauan Sekilas mengenai Fitur Sekuriti (Lanjutan)

Opsi	Uraian
Smart Cover	<p>Untuk:</p> <ul style="list-style-type: none"> • Memfungsikan/melumpuhkan Cover Lock. • Memfungsikan/melumpuhkan Cover Removal Sensor. <p> <i>Notify User</i> akan memberi peringatan pada pengguna bahwa sensor telah mendeteksi bahwa cover dilepas. <i>Setup Password</i> akan meminta agar pengguna memasukkan sandi setup untuk mem-boot komputer jika sensor mendeteksi bahwa cover telah dilepaskan.</p> <p>Fitur ini hanya didukung pada model-model tertentu saja. Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p>
Embedded Security	<p>Untuk:</p> <ul style="list-style-type: none"> • Memfungsikan/melumpuhkan perangkat Embedded Security. • Mengeset ulang perangkat ke setelan pabrik (Factory Settings). <p>Fitur ini hanya didukung pada model-model tertentu saja. Lihat <i>Panduan Sekuriti Tertanam HP ProtectTools</i>, pada <i>CD Dokumentasi</i> untuk informasi lebih lanjut.</p>
Device Security	Memfungsikan/melumpuhkan porta seri, porta paralel, porta USB depan, audio sistem, kontroler jaringan (model tertentu), perangkat MultiBay (model tertentu), dan kontroler SCSI (model tertentu).
Network Service Boot	Memfungsikan/melumpuhkan kemampuan komputer untuk mem-boot dari sistem operasi yang diinstal pada server jaringan. (Fitur tersedia pada model NIC saja; kontroler jaringan harus berada pada bus PCI atau tertanam pada system board.)
<p> Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada <i>CD Dokumentasi</i>.</p> <p>Dukungan untuk fitur sekuriti dapat bervariasi, bergantung pada konfigurasi komputer tersebut.</p>	




Tinjauan Sekilas mengenai Fitur Sekuriti *(Lanjutan)*

Opsi	Uraian
System IDs	<p>Untuk menyetel:</p> <ul style="list-style-type: none">• Tag aset (pengenal 18-bit) dan Tag kepemilikan (pengenal 80-bit yang ditampilkan dalam POST). <p>Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p> <ul style="list-style-type: none">• Nomor seri rangka (casis) atau nomor Universal Unique Identifier (UUID). UUID hanya dapat dimutakhirkan jika nomor seri rangka saat ini tidak valid. (Nomor ID ini biasanya diset di pabrik dan digunakan sebagai pengenal sistem tersebut.) <p>Setelan lokal papan ketik (misalnya, Bahasa Inggris atau Jerman) untuk entri System ID.</p>
DriveLock	<p>Untuk menetapkan atau mengubah sandi master atau sandi pengguna untuk hard drive (tidak didukung pada hard drive SCSI). Bila fitur ini difungsikan, pengguna akan diminta untuk memasukkan salah satu sandi DriveLock sewaktu POST berlangsung. Jika tidak ada sandi yang berhasil dimasukkan, hard drive akan tetap tidak dapat diakses hingga salah satu sandi berhasil dimasukkan saat proses cold-boot selanjutnya.</p> <p> Pemilihan ini hanya akan muncul bila pada sistem sedikitnya terpasang satu drive MultiBay yang mendukung fitur DriveLock.</p> <p>Lihat <i>Panduan Pemecahan Masalah</i> pada <i>CD Dokumentasi</i> untuk informasi lebih jauh.</p>
<p> Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada <i>CD Dokumentasi</i>.</p> <p>Dukungan untuk fitur sekuriti dapat bervariasi, bergantung pada konfigurasi komputer tersebut.</p>	

Tinjauan Sekilas mengenai Fitur Sekuriti *(Lanjutan)*

Opsi	Uraian
Master Boot Record Security	<p>Untuk memfungsikan atau melumpuhkan Master Boot Record (MBR) Security.</p> <p>Bila difungsikan, BIOS akan menolak semua permintaan untuk menuliskan MBR pada disk yang bisa di-boot saat ini. Setiap kali komputer dihidupkan atau di-boot ulang, BIOS akan membandingkan MBR dari disk yang dapat di-boot saat ini dengan MBR yang sebelumnya disimpan. Jika terdeteksi adanya perubahan, Anda dapat memilih apakah akan menyimpan MBR pada disk yang dapat di-boot saat ini, memulihkan MBR yang sebelumnya disimpan, atau melumpuhkan MBR Security. Anda harus mengetahui sandi penyiapan, jika ada.</p> <p> Sebelum mengganti format atau partisi pada disk yang bisa di-boot saat ini, lumpuhkan fitur MBR Security. Beberapa utilitas disk (seperti FDISK dan FORMAT) akan mencoba memutakhirkan MBR.</p> <p>Jika MBR Security difungsikan dan akses disk dilayani oleh BIOS, permintaan penulisan pada MBR akan ditolak, sehingga utilitas tersebut akan melaporkan galat.</p> <p>Jika MBR Security difungsikan dan akses disk dilayani oleh sistem operasi, perubahan MBR akan terdeteksi oleh BIOS selama boot-ulang berikutnya, dan pesan peringatan MBR Security akan ditampilkan.</p>
<p> Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada <i>CD Dokumentasi</i>.</p> <p>Dukungan untuk fitur sekuriti dapat bervariasi, bergantung pada konfigurasi komputer tersebut.</p>	

Tinjauan Sekilas mengenai Fitur Sekuriti (Lanjutan)

Opsi	Uraian
Save Master Boot Record	Menyimpan salinan cadangan dari Master Boot Record dari disk yang dapat di-boot saat ini. Hanya muncul jika MBR Security difungsikan.
Save Master Boot Record	Memulihkan cadangan Master Boot Record ke disk yang dapat di-boot saat ini.  Hanya muncul jika semua kondisi berikut dipenuhi: <ul style="list-style-type: none"> • MBR Security difungsikan. • Salinan cadangan MBR sudah disimpan sebelumnya. • Disk yang dapat di-boot saat ini adalah disk yang sama dengan yang digunakan untuk menyimpan salinan cadangan MBR tersebut.
	 AWAS: Memulihkan MBR yang sebelumnya disimpan setelah utilitas disk atau sistem operasi melakukan pengubahan MBR dapat menyebabkan data pada disk menjadi tidak dapat diakses. Lakukan pemulihan MBR simpanan tersebut hanya jika Anda yakin bahwa MBR pada disk boot sekarang telah mengandung kesalahan (corrupt) atau terinfeksi virus.
	Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada <i>CD Dokumentasi</i> . Dukungan untuk fitur sekuriti dapat bervariasi, bergantung pada konfigurasi komputer tersebut.

Pengamanan dengan Sandi

Sandi power-on (penyalan daya) berfungsi untuk mencegah penggunaan komputer oleh yang tidak berwenang, yakni dengan meminta sandi untuk mengakses aplikasi atau data setiap kali komputer dihidupkan atau dihidupkan ulang. Sandi penyiapan secara khusus mencegah akses yang tidak berwenang ke Computer Setup, dan juga dapat digunakan untuk mengganti (override) sandi power-on. Yaitu, bila komputer meminta sandi power-on, Anda dapat menggunakan sandi penyiapan sebagai gantinya untuk mengakses komputer.

Agar administrator sistem dapat log masuk ke semua sistem jaringan untuk melakukan perawatan tanpa harus mengetahui sandi power-on, walaupun sandi power-on sudah ditetapkan, dapat dibuat sandi penyiapan di seluruh jaringan.

Menetapkan Sandi Penyiapan Menggunakan Computer Setup

Jika sistem dilengkapi dengan perangkat sekuriti tertanam, lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi*. Penetapan sandi Supervisor melalui Computer Setup akan mencegah rekonfigurasi komputer (penggunaan utilitas Computer Setup F10) jika sandi belum dimasukkan.

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security**, kemudian pilih **Setup Password**, lalu ikuti petunjuk di layar.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Menetapkan Sandi Power-On Menggunakan Computer Setup

Penetapan sandi power-on melalui Computer Setup akan mencegah akses ke komputer saat komputer dihidupkan, jika sandi ini belum dimasukkan. Bila sandi power-on ditetapkan, Computer Setup menyediakan Password Options pada menu Security. Opsi-opsi sandi ini termasuk Password Prompt on Warm Boot. Bila Password Prompt on Warm Boot difungsikan, sandi juga harus dimasukkan setiap kali komputer di-boot ulang.

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security**, kemudian pilih **Power-On Password**, lalu ikuti petunjuk di layar.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Memasukkan Sandi Power-On

Untuk memasukkan sandi power-on, lakukan langkah-langkah berikut:

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart the Computer**.
2. Bila muncul ikon kunci pada monitor, ketikkan sandi saat ini, kemudian tekan **Enter**.



Ketikkan sandi dengan hati-hati; untuk alasan keamanan, karakter yang diketikkan tidak akan muncul di layar.

Jika Anda salah memasukkan sandi, akan muncul ikon kunci patah. Cobalah lagi. Jika Anda tiga kali gagal memasukkan sandi, Anda harus mematikan komputer, kemudian menghidupkannya lagi sebelum dapat melanjutkan.

Memasukkan Sandi Penyiapan

Jika sistem dilengkapi dengan perangkat sekuriti tertanam, lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi*.

Jika sandi penyiapan sudah ditetapkan pada komputer, Anda akan diminta untuk memasukkannya setiap kali Computer Setup dijalankan.

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Bila muncul ikon kunci pada monitor, ketikkan sandi saat ini, kemudian tekan **Enter**.



Ketikkan sandi dengan hati-hati; untuk alasan keamanan, karakter yang diketikkan tidak akan muncul di layar.

Jika Anda salah memasukkan sandi, akan muncul ikon kunci patah. Cobalah lagi. Jika Anda tiga kali gagal memasukkan sandi, Anda harus mematikan komputer, kemudian menghidupkannya lagi sebelum dapat melanjutkan.

Mengganti Sandi Power-On atau Sandi Penyiapan

Jika sistem dilengkapi dengan perangkat sekuriti tertanam, lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi*.

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart the Computer**.

2. Untuk mengganti sandi Power-On, lanjutkan ke langkah 3.

Untuk mengganti sandi Setup (penyiapan), segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Bila ikon kunci muncul, ketikkan sandi saat ini, garis miring (/) atau karakter pemisah lainnya, sandi baru, garis miring (/) atau karakter pemisah lainnya, kemudian sandi baru lagi sebagaimana ditunjukkan:
sandi saat ini/sandi baru/sandi baru



Ketikkan sandi dengan hati-hati; untuk alasan keamanan, karakter yang diketikkan tidak akan muncul di layar.

4. Tekan **Enter**.

Sandi baru ini akan berlaku pada saat berikutnya komputer dihidupkan.



Lihat [“Karakter Pemisah Papan Ketik Nasional”](#) pada halaman 34 untuk informasi mengenai karakter pemisah lain. Sandi power-on dan sandi penyiapan juga dapat diganti menggunakan opsi Security dalam Computer Setup.

Menghapus Sandi Power-On atau Sandi Penyiapan

Jika sistem dilengkapi dengan perangkat sekuriti tertanam, lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi*.

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart the Computer**.

2. Untuk menghapus sandi Power-On, lanjutkan ke langkah 3.

Untuk menghapus sandi Setup (penyiapan), segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Bila muncul ikon kunci, ketikkan sandi saat ini diikuti dengan garis miring (/) atau karakter pemisah lainnya, sebagaimana ditunjukkan:
sandi saat ini/

4. Tekan **Enter**.



Lihat “[Karakter Pemisah Papan Ketik Nasional](#)” untuk informasi mengenai karakter pemisah lain. Sandi power-on dan sandi penyiapan juga dapat diganti menggunakan opsi Security dalam Computer Setup.

Karakter Pemisah Papan Ketik Nasional

Setiap papan ketik dirancang untuk memenuhi ketentuan yang khas untuk setiap negara. Cara penulisan dan tombol yang digunakan untuk mengganti atau menghapus sandi bergantung pada papan ketik yang disertakan bersama komputer.

Karakter Pemisah Papan Ketik Nasional

Amerika Latin	-	Inggris U.K.	/	Rusia	/
Arab	/	Italia	-	Slovakia	-
Belgia	=	Jepang	/	Spanyol	-
BHKSY*	-	Jerman	-	Swedia/Finlandia	/
Brazilia	/	Korea	/	Swiss	-
Ceko	-	Norwegia	-	Taiwan	/
Cina	/	Perancis	!	Thai	/
Denmark	-	Perancis Kanada	é	Turki	.
Hungaria	-	Polandia	-	Yahudi	.
Inggris A.S.	/	Portugis	-	Yunani	-

* Untuk Bosnia-Herzegovina, Kroasia, Slovenia, dan Yugoslavia

Mengosongkan Sandi

Jika Anda lupa sandinya, Anda tidak dapat mengakses komputer. Lihat *Panduan Pemecahan Masalah* pada *CD Dokumentasi* untuk instruksi mengenai pengosongan sandi.

Jika sistem dilengkapi dengan perangkat sekuriti tertanam, lihat *Panduan Sekuriti Tertanam HP ProtectTools*, pada *CD Dokumentasi*.

DriveLock

DriveLock adalah fitur keamanan standar-industri yang mencegah akses tak berwenang ke data pada hard drive MultiBay. DriveLock diterapkan sebagai perluasan dari Computer Setup. Fitur ini hanya tersedia jika terdeteksi adanya hard drive yang dapat difungsikan dengan DriveLock.

DriveLock ditujukan bagi pelanggan HP yang sangat mementingkan keamanan data. Bagi pelanggan seperti itu, biaya hard drive dan hilangnya data yang disimpan di dalamnya tidaklah berarti dibanding dengan kerusakan yang dapat disebabkan jika isi hard drive diakses oleh yang tidak berhak. Untuk mencari keseimbangan antara tingkat keamanan ini dengan kebutuhan praktis jika ada sandi yang terlupakan, maka penerapan DriveLock oleh HP menggunakan skema keamanan dua-sandi. Satu sandi ditujukan untuk ditetapkan dan digunakan oleh administrator sistem, sementara sandi lainnya biasanya ditetapkan dan digunakan oleh pengguna-akhir. Jika kedua sandi ini hilang, tidak ada “pintu belakang” yang dapat digunakan untuk membuka kunci drive. Oleh karena itu, DriveLock paling aman digunakan bila data yang terdapat pada hard drive dibuat replikanya pada suatu sistem informasi perusahaan, atau secara berkala dibuatkan cadangannya.

Jika kedua sandi DriveLock ini hilang, maka hard drive tidak dapat digunakan lagi. Untuk pengguna yang profilnya tidak sesuai dengan profil pelanggan yang diuraikan sebelumnya, ini mungkin bukan merupakan risiko yang dapat diterima. Untuk pengguna yang profilnya sesuai dengan yang diuraikan di atas, risiko ini dapat ditolerir mengingat sifat data yang tersimpan pada hard drive tersebut.

Menggunakan DriveLock

Opsi DriveLock terdapat pada menu Security dalam Computer Setup. Pengguna diberi pilihan untuk menetapkan sandi master atau untuk memfungsikan DriveLock. Sandi pengguna harus diberikan agar dapat memfungsikan DriveLock. Karena konfigurasi awal DriveLock biasanya dilakukan oleh administrator sistem, maka terlebih dahulu harus ditetapkan sandi master. HP menyarankan administrator sistem untuk menetapkan sandi master, tanpa melihat apakah DriveLock akan difungsikan atau dilumpuhkan. Dengan demikian, administrator dapat memodifikasi setelan DriveLock jika drive terkunci di lain waktu. Setelah sandi master ditetapkan, administrator sistem dapat memfungsikan DriveLock atau tetap membiarkannya dalam keadaan dilumpuhkan.

Jika ada hard drive yang terkunci, POST akan meminta sandi untuk membuka kunci perangkat tersebut. Jika sandi power-on sudah ditetapkan dan sama dengan sandi pengguna perangkat tersebut, POST tidak akan meminta pengguna untuk memasukkan lagi sandi tersebut. Jika tidak, pengguna akan diminta untuk memasukkan sandi DriveLock. Salah satu dari sandi master atau sandi pengguna dapat digunakan. Pengguna memiliki kesempatan dua kali untuk memasukkan sandi yang benar. Jika kedua upaya ini tidak berhasil, POST akan dilanjutkan, namun drive tersebut tetap tidak dapat diakses.

Aplikasi DriveLock

Penggunaan paling praktis dari fitur keamanan DriveLock adalah pada lingkungan perusahaan di mana administrator sistem menyediakan hard drive MultiBay untuk digunakan pada sebagian komputer. Administrator sistem bertanggung jawab untuk mengkonfigurasi hard drive MultiBay tersebut. Kegiatan ini di antaranya mencakup menetapkan sandi master DriveLock. Jika sandi pengguna terlupakan atau perangkat tersebut dialihkan ke karyawan lain, sandi master selalu dapat digunakan untuk menyetel ulang sandi pengguna sehingga hard drive kembali dapat diakses.


HP menyarankan agar administrator sistem perusahaan yang memilih untuk memfungsikan DriveLock juga menetapkan suatu kebijakan perusahaan untuk menetapkan dan menyelenggarakan sandi master. Ini harus dilakukan untuk mencegah situasi di mana seorang karyawan, baik sengaja ataupun tidak, menetapkan kedua sandi DriveLock sebelum keluar dari perusahaan tersebut. Dalam keadaan tersebut, hard drive tidak dapat dipakai lagi sehingga harus diganti. Sebaliknya, jika sandi master tidak ditetapkan, administrator sistem dapat terjebak pada keadaan di mana hard drive terkunci dan ia tidak dapat melakukan pemeriksaan rutin atas perangkat lunak yang tak diizinkan, fungsi-fungsi pengontrolan aset lainnya, serta memeriksa ketersediaan dukungan.

Untuk pengguna yang kebutuhan keamanannya tidak setinggi itu, HP tidak menyarankan untuk memfungsikan DriveLock. Pengguna dalam kategori ini mencakup pengguna pribadi atau pengguna yang biasanya tidak memiliki data sensitif pada hard drive-nya. Bagi pengguna jenis ini, kerugian akibat hilangnya hard drive akibat terlupanya kedua sandi jauh lebih besar dari nilai data yang dilindungi oleh DriveLock. Akses ke Computer Setup dan DriveLock dapat dibatasi melalui sandi Setup (penyiapan). Dengan menetapkan sandi Setup dan tidak memberikannya kepada pengguna akhir, administrator dapat membatasi pengguna agar tidak memfungsikan DriveLock.

Smart Cover Sensor

Cover Removal Sensor, yang tersedia pada model-model tertentu, adalah kombinasi antara teknologi perangkat keras dan perangkat lunak yang dapat memberi peringatan jika penutup komputer atau panel samping dilepaskan. Ada tiga tingkat perlindungan, sebagaimana diuraikan dalam tabel berikut.

Tingkat perlindungan Smart Cover Sensor

Tingkat	Setelan	Uraian
Level 0	Disabled	Smart Cover Sensor dilumpuhkan (default).
Level 1	Notify User	Bila komputer dihidupkan ulang, layar menampilkan pesan yang menunjukkan bahwa tutup komputer atau panel samping terlepas.
Level 2	Setup Password	Bila komputer dihidupkan ulang, layar menampilkan pesan yang menunjukkan bahwa tutup komputer atau panel samping terlepas. Anda harus memasukkan sandi penyiapan untuk melanjutkan.
 Setelan ini dapat diubah dengan menggunakan Computer Setup. Untuk informasi lebih lanjut mengenai Computer Setup, lihat <i>Panduan Utilitas Penyiapan Komputer (F10)</i> pada CD Dokumentasi.		

Menetapkan Tingkat Perlindungan Smart Cover Sensor

Untuk menetapkan tingkat perlindungan Smart Cover Sensor, ikuti langkah-langkah berikut:

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security > Smart Cover > Cover Removal Sensor**, kemudian tetapkan tingkat perlindungan yang dikehendaki.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Smart Cover Lock

The Smart Cover Lock adalah pengunci tutup komputer yang dikontrol oleh perangkat lunak, dan tersedia pada komputer HP tertentu. Kunci ini berfungsi mencegah agar komponen internal tidak diakses oleh yang tidak berhak. Komputer ini dijual dengan Smart Cover Lock dalam posisi tidak terkunci.



AWAS: Untuk keamanan kunci tutup komputer yang maksimum, pastikan untuk menetapkan sandi penyiapan. Sandi penyiapan ini mencegah agar utilitas Computer Setup tidak diakses oleh yang tidak berhak.



Smart Cover Lock tersedia sebagai pilihan pada sistem-sistem tertentu.

Mengunci Smart Cover Lock

Untuk mengaktifkan dan mengunci Smart Cover Lock, lakukan langkah-langkah berikut:

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih opsi **Security > Smart Cover > Cover Lock > Lock**.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Membuka Kunci Smart Cover Lock

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security > Smart Cover > Cover Lock > Unlock**.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Menggunakan Smart Cover FailSafe Key

Jika Anda memfungsikan Smart Cover Lock dan tidak dapat memasukkan sandi untuk melumpuhkan kunci tersebut, Anda memerlukan Smart Cover FailSafe Key untuk membuka tutup komputer. Anda memerlukan kunci ini dalam kondisi-kondisi berikut:

- Listrik mati
- Kegagalan startup
- Kegagalan komponen PC (misalnya prosesor atau catu daya)
- Sandi terlupakan



AWAS: Smart Cover FailSafe Key adalah alat bantu khusus yang dapat diperoleh dari HP. Bersiaplah, pesanlah kunci ini pada penjual atau penyedia layanan resmi, sebelum Anda membutuhkannya.

Untuk mendapatkan FailSafe Key, lakukan salah satu dari hal-hal berikut:

- Hubungi penjual atau penyedia layanan resmi HP.
- Hubungi nomor telepon yang sesuai, yang tercantum pada jaminan.

Untuk informasi lebih jauh mengenai cara menggunakan Smart Cover FailSafe Key, lihat *Panduan Referensi Perangkat Keras* pada *CD Dokumentasi*.

Master Boot Record Security

Master Boot Record (MBR) berisi informasi yang diperlukan agar komputer dapat mem-boot dari disk dan untuk mengakses data yang disimpan dalam disk. Master Boot Record Security berfungsi mendeteksi dan melaporkan perubahan yang tidak dikehendaki atau perubahan yang berbahaya pada MBR, seperti yang diakibatkan oleh sejumlah virus komputer atau oleh penggunaan utilitas disk tertentu secara tidak benar. Dengan MBR, Anda juga dapat memulihkan MBR “terakhir yang diketahui masih baik”, jika perubahan pada MBR terdeteksi ketika sistem dimulai.

Untuk memfungsikan sekuriti MBR, lakukan langkah-langkah berikut:

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security > Master Boot Record Security > Enabled**.
4. Pilih **Security > Save Master Boot Record**.
5. Sebelum keluar, klik **File > Save Changes and Exit**.

Bila MBR Security difungsikan, BIOS akan mencegah agar tidak ada perubahan pada MBR dari disk yang dapat di-boot saat ini, ketika sistem sedang dalam mode MS-DOS atau Windows Safe Mode.



Sebagian besar sistem operasi mengontrol akses ke MBR dari disk yang dapat di-boot saat ini; BIOS tidak dapat mencegah perubahan yang mungkin terjadi saat sistem operasi dijalankan.

Setiap kali komputer dihidupkan atau dihidupkan ulang, BIOS akan membandingkan MBR dari disk yang dapat di-boot saat ini dengan MBR yang sebelumnya disimpan. Jika terdeteksi adanya perubahan dan jika disk yang dapat di-boot saat ini adalah disk yang merupakan tempat penyimpanan MBR sebelumnya, maka pesan berikut akan ditampilkan:

1999 — Master Boot Record has changed.

Tekan sembarang tombol untuk memasuki Setup
(Penyiapan) untuk mengkonfigurasi MBR Security.

Setelah memasuki Computer Setup, Anda harus

- Menyimpan MBR dari disk yang saat ini dapat di-boot;
- Memulihkan MBR yang sebelumnya disimpan; atau
- Melumpuhkan fitur MBR Security.

Anda harus mengetahui sandi penyiapan, jika ada.

Jika terdeteksi adanya perubahan dan jika disk yang dapat di-boot saat ini **bukan** merupakan disk yang menjadi tempat penyimpanan MBR sebelumnya, maka pesan berikut akan ditampilkan:

2000 — Master Boot Record Hard Drive has changed.

Tekan sembarang tombol untuk memasuki Setup
(Penyiapan) untuk mengkonfigurasi MBR Security.

Setelah memasuki Computer Setup, Anda harus

- Menyimpan MBR dari disk yang saat ini dapat di-boot; atau
- Melumpuhkan fitur MBR Security.

Anda harus mengetahui sandi penyiapan, jika ada.

Jika MBR yang sebelumnya disimpan ternyata mengandung kesalahan (corrupt), di mana hal ini sangat kecil kemungkinannya, maka pesan berikut akan ditampilkan:

1998 — Master Boot Record has been lost.

Tekan sembarang tombol untuk memasuki Setup
(Penyiapan) untuk mengkonfigurasi MBR Security.

Setelah memasuki Computer Setup, Anda harus

- Menyimpan MBR dari disk yang saat ini dapat di-boot; atau
- Melumpuhkan fitur MBR Security.

Anda harus mengetahui sandi penyiapan, jika ada.

Sebelum Memformat atau Memasang Partisi pada Disk yang Dapat Di-boot Saat Ini

Pastikan MBR Security dilumpuhkan sebelum Anda mengganti partisi atau format disk yang dapat di-boot saat ini. Beberapa utilitas disk, seperti FDISK dan FORMAT, akan mencoba memutakhirkan MBR. Jika MBR security difungsikan ketika Anda mengganti partisi atau format disk, Anda mungkin menerima pesan galat dari utilitas disk atau peringatan dari MBR Security, setiap kali komputer dihidupkan atau dihidupkan ulang. Untuk melumpuhkan MBR Security, lakukan langkah-langkah berikut:

1. Hidupkan atau hidupkan ulang komputer. Jika Anda menggunakan Windows, klik **Start > Shut Down > Restart**.
2. Segera setelah komputer dihidupkan, tekan terus tombol **F10** sampai masuk ke Computer Setup. Tekan **Enter** untuk melewati layar judul, jika perlu.



Jika Anda tidak menekan tombol **F10** pada saat yang tepat, Anda harus menghidupkan ulang komputer, lalu kembali menekan terus tombol **F10** untuk dapat mengakses utilitas tersebut.

Jika Anda menggunakan papan ketik PS/2, mungkin muncul pesan Keyboard Error — abaikan saja.

3. Pilih **Security > Master Boot Record Security > Disabled**.
4. Sebelum keluar, klik **File > Save Changes and Exit**.

Pemasangan Kunci Kabel

Pada panel belakang komputer dapat dipasang kunci kabel sehingga fisik komputer dapat dikunci ke suatu area kerja.

Untuk petunjuk yang disertai ilustrasi, lihat *Panduan Referensi Perangkat Keras* pada *CD Dokumentasi*.

Teknologi Identifikasi Sidik Jari

Dengan menghilangkan kebutuhan untuk memasukkan sandi pengguna, HP Fingerprint Identification Technology berfungsi mengetatkan keamanan jaringan, menyederhanakan proses log masuk, dan mengurangi biaya pengelolaan jaringan perusahaan. Dengan harga yang terjangkau, fitur ini tidak lagi tersedia hanya untuk organisasi berteknologi tinggi dengan tingkat keamanan tinggi.



Dukungan bagi Fingerprint Identification Technology bervariasi berdasarkan model.

Untuk informasi lebih jauh, kunjungi:

<http://h18004.www1.hp.com/products/security/>.

Pemberitahuan dan Pemulihan Kesalahan

Fitur Fault Notification and Recovery (Pemberitahuan dan Pemulihan Kesalahan) menggabungkan teknologi perangkat keras dan perangkat lunak untuk mencegah hilangnya data kritis dan untuk meminimasi waktu non-operasi (downtime) yang tidak direncanakan.

Jika komputer terhubung ke jaringan yang dikelola oleh HP Client Manager, komputer akan mengirimkan pemberitahuan kesalahan kepada aplikasi manajemen jaringan. Dengan HP Client Manager Software, Anda juga dapat melakukan penjadwalan Diagnostics secara jarak jauh, agar Diagnostics otomatis dijalankan pada semua PC yang dikelola, dan membuat laporan ikhtisar tes yang gagal.

Sistem Perlindungan Drive

Drive Protection System (sistem perlindungan drive atau DPS) adalah sebuah alat bantu diagnostik yang dipasang pada hard drive yang terdapat pada komputer HP tertentu. DPS dirancang untuk membantu mendiagnosis masalah yang mungkin muncul akibat penggantian hard drive yang tidak dikehendaki.

Ketika komputer HP dibuat, setiap hard drive yang terpasang dites dengan menggunakan DPS, dan sebuah catatan permanen mengenai informasi penting dituliskan pada drive tersebut. Setiap kali DPS dijalankan, hasil tes dituliskan pada hard drive. Penyedia layanan dapat menggunakan informasi ini untuk membantu mendiagnosis kondisi yang menyebabkan Anda menjalankan perangkat lunak DPS tersebut. Lihat *Panduan Pemecahan Masalah* pada *CD Dokumentasi* untuk instruksi mengenai cara menggunakan DPS.

Catu Daya yang Dapat Menahan Lonjakan Arus

Dengan catu daya terpadu yang dapat menahan lonjakan arus, komputer menjadi lebih handal bila terkena lonjakan arus yang tak terduga. Catu daya ini dapat menahan lonjakan arus listrik hingga 2000 volt tanpa menyebabkan terhentinya operasi atau kehilangan data.

Sensor Panas

Sensor panas adalah fitur perangkat keras dan perangkat lunak yang berfungsi menelusuri suhu bagian dalam komputer. Fitur ini menampilkan pesan peringatan bila rentang normal sudah terlampaui, sehingga Anda punya cukup waktu untuk bertindak sebelum komponen internal menjadi rusak atau data rusak.

Indeks

A

akses ke komputer, mengontrol 23
Alamat Internet, Lihat situs Web
alat bantu cloning, perangkat lunak 2
alat bantu diagnostik untuk hard drive 46
alat bantu penerapan, perangkat lunak 2
Altiris 4

C

catu daya yang tahan lonjakan arus 46
catu daya, tahan lonjakan arus 46
Computer Setup Utilities 10
cover lock, smart 39

D

disk yang dapat di-boot, informasi penting 44
disk, cloning 2
DiskOnKey
 lihat juga HP Drive Key
 yang dapat di-boot 14~20
drive, melindungi 46
Drivelock 35~37

F

FailSafe Boot Block ROM 9
FailSafe Key
 memesan 41
 peringatan 41

H

hard drive, alat bantu diagnostik 46
HP Client Manager 4
HP Drive Key
 lihat juga DiskOnKey
 yang dapat di-boot 14~20

I

image perangkat lunak pra-instal, melakukan
 kustomisasi perangkat lunak, perangkat
 lunak
 integrasi 2

K

karakter pemisah papan ketik nasional 34
karakter pemisah papan ketik, nasional 34
karakter pemisah, tabel 34
keamanan
 DriveLock 35~37
 MultiBay 35~37
 sandi 29
 Smart Cover Lock 39~41
 Smart Cover Sensor 38
keamanan kunci tutup komputer,
 peringatan 39
keamanan Multibay 35~37
konfigurasi awal 2

L

lampu papan ketik, ROM, tabel 10

M

- Master Boot Record Security 42~43
- melindungi hard drive 46
- melindungi ROM, peringatan 7
- memasang partisi disk, informasi penting 44
- memasukkan
 - sandi penyiapan 31
 - sandi power-on 30
- membuka kunci Smart Cover Lock 40
- memesan FailSafe Key 41
- memformat disk, informasi penting 44
- memulihkan sistem 8
- mengganti sandi 32
- mengganti sistem operasi, informasi penting 22
- menghapus sandi 33
- mengkongfigurasi tombol daya 21
- mengontrol akses ke komputer 23
- mengosongkan sandi 34
- mengunci Smart Cover Lock 40
- meningkatkan ROM 7

P

- PCN (Proactive Change Notification) 6
- pemasangan kunci kabel 44
- pemberitahuan kesalahan 45
- pemberitahuan perubahan 6
- pemulihan sistem 8
- pemulihan, perangkat lunak 2
- penelusuran aset 23
- penyiapan
 - awal 2
 - membuat replika 10
- penyiapan jarak jauh 3
- perangkat lunak
 - Computer Setup Utilities 10
 - Drive Protection System 46
 - FailSafe Boot Block ROM 9
 - Fault Notification and Recovery 45

- Master Boot Record Security 42~43
- memutakhirkan lebih dari satu mesin 6
- pemulihan 2
- penelusuran aset 23
- Remote ROM Flash 8
- Remote System Installation 3
- System Software Manager 6
- perangkat media flash USB, yang dapat di-boot 14~20
- perangkat yang dapat di-boot
 - DiskOnKey 14~20
 - HP Drive Key 14~20
 - membuat 14~20
 - perangkat media flash USB 14~20
- peringatan
 - FailSafe Key 41
 - keamanan kunci tutup komputer 39
 - melindungi ROM 7
- Preboot Execution Environment (PXE) 3
- Proactive Change Notification (PCN) 6
- PXE (Preboot Execution Environment) 3

R

- Remote ROM Flash 8
- Remote System Installation, mengakses 3
- ROM
 - lampu papan ketik, tabel 10
 - peningkatan 7
 - Remote Flash 8
- ROM sistem tidak valid, ROM tidak valid 9

S

- sandi
 - keamanan 29
 - mengganti 32
 - menghapus 33
 - pengosongan 34
 - penyiapan 29, 31
 - power-on 30

- sandi penyiapan
 - memasukkan 31
 - mengganti 32
 - menghapus 33
 - setelan 29
 - sandi power-on
 - memasukkan 30
 - mengganti 32
 - menghapus 33
 - sekuriti
 - fitur, tabel 24
 - Master Boot Record 42~43
 - setelan, penyiapan 23
 - sensor panas 46
 - sistem operasi, informasi penting tentang 22
 - situs Web
 - Altiris 5
 - dukungan perangkat lunak 22
 - Fingerprint Identification Technology 45
 - HP Client Manager 4
 - HPQFlash 8
 - image ROMPaq 7
 - membuat replika konfigurasi penyiapan 13, 14
 - Proactive Change Notification 6
 - Remote ROM Flash 8
 - ROM Flash 7
 - Subscriber's Choice 7
 - System Software Manager (SSM) 6
 - situs web
 - penerapan PC 2
 - Smart Cover FailSafe Key, memesan 41
 - Smart Cover Lock 39~41
 - membuka kunci 40
 - mengunci 40
 - Smart Cover Sensor 38
 - setelan, 39
 - tingkat perlindungan 38
 - SSM (System Software Manager) 6
 - suhu bagian dalam komputer 46
 - suhu, bagian dalam komputer 46
 - System Software Manager (SSM) 6
- T**
- teknologi identifikasi sidik jari 45
 - tombol daya
 - fungsi ganda 21
 - mengkonfigurasi 21
 - tombol daya fungsi ganda 21
- U**
- URL (situs Web). Lihat situs Web